Title	ブール多項式環上のグレブナー基底の諸性質について(数式処理における理論とその応用の研究)
Author(s)	佐藤, 洋祐
Citation	数理解析研究所講究録 (1995), 920: 53-61
Issue Date	1995-08
URL	http://hdl.handle.net/2433/59718
Right	
Type	Departmental Bulletin Paper
Textversion	publisher

数理解析研究所講究録
920巻 1995年 53-61

6.

ブール多項式環上のグレブナー基底の諸性質について

佐藤 洋祐 (立命館大理工)

6.1 はじめに

ブール環 B を係数環とする多項式環 $\mathbf{B}[X_1,\ldots,X_n]$ において, ブール環固有の性質を使って多項式による単項リダクションが定義され, これを用いて $\mathbf{B}[X_1,\ldots,X_n]$ におけるグレブナー基底がBuchberger のアルゴリズムと同様の完備化手続きに基づくアルゴリズムによって求めることができる.([Sakai 88,90],[Weispfenning 89]) 本稿ではこのグレブナー基底が持ついくつかの性質について紹介する. 以下ではまず 2 節で $\mathbf{B}[X_1,\ldots,X_n]$ における単項リダクションとグレブナー基底について概説する. 次に 3 節で syzygy 基底との関係とアルゴリズムの効率化,4 節で comprehensive グレブナー基底の構成について述べ,5 節で集合制約ソルバーへの応用を紹介する.

6.2 ブーリアン・グレブナー基底

単位元 1 を持つ可換環 B は, すべての元がベキ等元になるとき, すなわち

$$\forall a \in \mathbf{B} \quad a^2 = a.$$

をみたすとき, ブール**環** と呼ばれ, 次の性質を持つ.

$$\forall a \in \mathbf{B} \quad a + a = 0.$$

以下では, 与えられたブール環 $\mathbf{B}$ を係数環とする多項式環 $\mathbf{B}[X_1, X_2, \ldots, X_n]$ を考える. $\mathbf{B}$ の要素を表す文字として a, b, c, ... を, $X_1, X_2, \ldots, X_n$ からなる項を表す文字として α, β, γ, ... を使う.
$>$ をアドミシブルな全順序 (admissible ordering), すなわち

1. $\alpha > \beta$ ならば任意の項 γ にたいして $\alpha\gamma > \beta\gamma$.
2. 1 と異なる任意の項 α にたいして $\alpha > 1$.

が成り立つとする.
多項式 f の順序最大の項 (最大項) を $lpp(f)$ で, その係数を $lc(f)(\in\mathbf{B})$ で, さらに f からその最大単項すなわち $lc(f)lpp(f)$ を取り除いた残りの部分を $res(f)$ でそれぞれ表す.
多項式 f にたいし, $lc(f) = a$,$lpp(f) = \alpha$,$res(f) = h$ であるとき, f を記号 $a\alpha \triangleright h$ で表すものとする.

多項式 $f = a\alpha \triangleright h$ による多項式上の**単項リダクション** (M-reduction, 以下では単にリダクションと呼ぶ) $\rightarrow_f$ を以下のように定義する.

$$b\alpha\gamma + g \rightarrow_f (1+a)b\alpha\gamma + abh\gamma + g.$$

ただし, ここで多項式 $b\alpha\gamma + g$ は $ab \neq 0$ をみたすものに限定する. (注意. $f = 0$ なら $a\alpha = h$, 両辺に a をかけると $a\alpha = ah$ となる. またブール環では $-$(マイナス) は扱わないが, 仮に $-$ を用いれば $a + a = 0$ より $(1+a) = (1-a)$ となるが, この形にすると上式の意味は明白であろう.)

F を多項式の集合とする. F によるリダクション $\rightarrow_F$ を F に含まれるあるルールによるリダクションすなわち $h \rightarrow_F h' \Leftrightarrow \exists f \in F\ h \rightarrow_f h'$ で定義する. $\rightarrow_F$ の推移反射閉包を $\stackrel{*}{\rightarrow}_F$ で表す. F が有限集合のとき $\rightarrow_F$ は停止性を持つ, すなわち無限に続く多項式のリダクション $f_0 \rightarrow_F f_1 \rightarrow_F f_2 \cdots$ は存在しない. (無限集合の場合には $\rightarrow_F$ は一般に停止性は持たない.) 多項式 f と g が $f \stackrel{*}{\rightarrow}_F g$ かつ g は F の任意の要素でリダクションできないとき, g は f の $\rightarrow_F$ による**既約形**であるという. $\rightarrow_F$ による f の既約形は一般には一つ以上存在するが $f\downarrow_F$ でそのうちの一つを表す.

I を $\mathbf{B}[X_1, X_2, \ldots, X_n]$ のイデアルとする. ルール多項式の有限集合 G が以下の性質をみたすとき, G は I のブーリアン・グレブナー**基底**と呼ばれる.

1. I は G で生成されるイデアルである.
2. $g + g' \in I \Leftrightarrow$ ある多項式 h が存在して $g \stackrel{*}{\rightarrow}_G h$ かつ $g' \stackrel{*}{\rightarrow}_G h$ が成り立つ.
   (特に $g \in I \Leftrightarrow g \stackrel{*}{\rightarrow}_G 0$.)

多項式 f と g にたいし以下で定義される多項式を f と g の **S 多項式**と呼び $\mathrm{sp}(f,g)$ と表す.

$$\mathrm{sp}(f,g) = lc(g)\frac{lpp(g)}{\mathrm{GCD}(lpp(f),lpp(g))}f + lc(f)\frac{lpp(f)}{\mathrm{GCD}(lpp(f),lpp(g))}g$$

ここで $\mathrm{GCD}(lpp(f), lpp(g))$ は項 $lpp(f)$ と $lpp(g)$ の最大公約項を表す.
多項式 h にたいし以下で定義される多項式をその**自己 C 多項式**と呼び $\mathrm{scp}(h)$ で表す.

$$\mathrm{scp}(h) = (1 + lc(h))h$$

ブーリアン・グレブナー基底は次のように特徴付けられる.

定理 1　多項式の有限集合 G は, $\mathrm{GCD}(lpp(f), lpp(g)) \neq 1$ なる任意の多項式 $f, g \in G$ にたいして $\mathrm{scp}(f) \stackrel{*}{\rightarrow}_G 0$ および $\mathrm{sp}(f,g) \stackrel{*}{\rightarrow}_G 0$ が成り立つとき, かつそのときに限りブーリアン・グレブナー

基底になる. □

与えられた多項式の有限集合 Fにたいし, Fで生成されるイデアルのブーリアン・グレブナー基底を求めるアルゴリズムは以下のように与えられる.

input $E \longleftarrow F, R \longleftarrow \emptyset$
  while $E \neq \emptyset$
    choose $h \in E$
      if $h\downarrow_R = 0$
        then
        $E \longleftarrow E - \{h\}$
        else let $f = h\downarrow_R$ **and**
        $E \longleftarrow (E - \{h\}) \cup \{\mathrm{scp}(f)\} \cup$
            $\{\mathrm{sp}(lc(f)f, g) \mid g \in R$
              $, \mathrm{GCD}(lpp(f), lpp(g)) \neq 1\}$
        $R \longleftarrow R \cup \{lc(f)f\}$
      end-if
  end-while
output R

Rが求めるブーリアン・グレブナー基底である.

6.3 syzygy基底とアルゴリズムの効率化

m 個の単項の列 $M = (a_1\alpha_1, a_2\alpha_2, \ldots, a_m\alpha_m)$ に対し$\sum_{i=1}^{m} a_i\alpha_i h_i = 0$ となるような m 個の多項式の列 $(h_1, h_2, \ldots, h_m)$ を Mの **syzygy** と呼ぶ. 特に, すべての h_i が単項で, そのうち 0 でないもの $h_{l_1}, \ldots, h_{l_k}$ に対して, $lpp(h_{l_1})\alpha_{l_1} = \cdots = lpp(h_{l_k})\alpha_{l_k}$が成り立つとき, **homogeneous** な **syzygy** と呼ぶ. Mの syzygy の全体は明らかにモデュールを形成するが, これを S_Mで表す.

通常のグレナー基底の場合と同様に syzygy のことばで定理 1 は次のように一般化することができる.

定理 2　$G = \{g_1, \ldots, g_m\}$ を多項式の有限集合, Mを G のすべての要素の最大単項をこの順に列べたもの, L を S_Mの homogeneous な基底とする. このとき, L のあらゆる元 $(h_1, \ldots, h_m)$ にたいして$\sum_{i=1}^{m} h_i g_i \stackrel{*}{\rightarrow}_G 0$ が成り立つとき, かつそのときに限り G はブーリアン・グレブナー基底になる. □

これが実際に一般化になっているのは次のことからみることができる.

$m(>2)$ 個の単項の列 $(a_1\alpha_1, \ldots, a_m\alpha_m)$ を Mとおく. $1 \leq i < j < k \leq m$ なる自然数 i, j, kにたいし

$$\alpha_{ij} = \mathrm{LCM}(\alpha_i, \alpha_j), \qquad \alpha_{ijk} = \mathrm{LCM}(\alpha_i, \alpha_j, \alpha_k),$$

とおく. ここで LCM は最小公倍項を表す. さらに

$$C_{ij} = \frac{a_j \alpha_{ij}}{\alpha_i} \vec{e}_i + \frac{a_i \alpha_{ij}}{\alpha_j} \vec{e}_j, \qquad C_i = (1 + a_i)\vec{e}_i,$$

とおく. ここで$\vec{e}_i$は i 番目の成分が 1 で残りの成分は 0 であるような m 個の列を表す.

定理 3 $L = \{C_{ij} | \, 1 \leq i < j \leq m\} \cup \{C_i | \, 1 \leq i \leq m\}$ とおくと, L は S_M の homogeneous な基底になる. □

多項式の集合 F（適当に列べられているとする）にたいする S 多項式は, 通常は Fの単項の列の syzygy 全体から成るモデュールの基底の元と Fの内積として定義される. 例えば係数環が体のとき,Buchberger によって与えられた S 多項式はモデュールの基底として Tayler 基底を用いたもので, これの特殊なケースにあたる.

m 個の多項式の列 $(a_1\alpha_1 \triangleright h_1, \ldots, a_m\alpha_m \triangleright h_m)$ を Fとおく. このとき, $a_i\alpha_i \triangleright h_i$の自己 C 多項式は, 上の記号を使うと $F \cdot C_i$と表され, 通常の S 多項式の一種であることがわかる.

さて homogeneous な基底に関して次のことが成り立つ.

定理 4 $1 \leq k \leq l$なるあらゆる kにたいし$\alpha_{n_k} | \alpha_{ij}$であり, さらに $(a_{n_1} \vee a_{n_2} \cdots \vee a_{n_l}) a_i a_j = a_i a_j$ が成り立つとき, C_{ij}は $C_{in_1}, C_{in_2}, \ldots, C_{in_l}, C_{jn_1}, C_{jn_2}, \ldots, C_{jn_l}, C_i, C_j$ の線形和として表される. (ここで記号$\vee$はブール代数の和を表す. すなわち $a \vee b = a + b + ab$.) □

これにより不要な S 多項式の計算を除去することによって, ブーリアン・グレブナー基底を求めるアルゴリズムを, 次のように改良できる.

Fを多項式の有限集合とする.

input $E \longleftarrow F, R \longleftarrow \emptyset$
  while $E \neq \emptyset$
    choose $h \in E$
      if $h\downarrow_R = 0$
        then
        $E \longleftarrow E - \{h\}$
        else let $f = h\downarrow_R$ and
        $E \longleftarrow (E - \{h\}) \cup \{\mathrm{scp}(f)\} \cup$
            $\{\mathrm{cp}(lc(f)f, g) | \, g \in R, \neg \mathrm{Red}(f, g, R)\}$
        $R \longleftarrow R \cup \{lc(f)f\}$
      end-if
  end-while
output R

Rは Fで生成されるイデアルのブーリアン・グレブナー基底になる.

Red(f,g,R) は不要な S 多項式の計算を除去するためのもので, 以下のいずれかの場合に限って真となる.

場合 1) GCD$(lpp(f),lpp(g))=1$;

場合 2) Rの中に $lc(f)f$ と gのどちらとも異なる多項式 $h_1,\ldots h_l$ があって, それぞれにたいして

$lpp(h_i)|$LCM$(lpp(f),lpp(g))$ が成り立ち, かつ

$(lc(h_1)\vee\cdots\vee lc(h_l))lc(f)lc(g)=lc(f)lc(g)$ となる.

6.4 comprehensiveグレブナー基底

多項式環 $\mathbf{B}[X_1,X_2,\ldots,X_n]$ はそれ自身ブール環にはならないが各変数 $X_1,X_2,\ldots,X_n$ をベキ等にすることによってブール環になる. すなわちイデアル $(X_1^2+X_1,X_2^2+X_2,\ldots,X_n^2+X_n)$ による剰余環 $\mathbf{B}[X_1,X_2,\ldots,X_n]/(X_1^2+X_1,X_2^2+X_2,\ldots,X_n^2+X_n)$ は再びブール環になる. 以後このブール環を $\mathbf{B}(X_1^2+X_1,X_2^2+X_2,\ldots,X_n^2+X_n)$ で表す. この剰余環においてもブーリアン・グレブナー基底が自然に導入されるが, 以下では特にことわらない限りブーリアン・グレブナー基底は剰余環上のものを, また剰余環上のリダクションや既約形等の記号も, もとの記号をそのまま使うことにする.

さて剰余環上で考えると comprehensive なグレブナー基底 ([Weispfenning 92]) が容易に構成することができることが以下のようにいえる.

I を $B(\bar{X},\bar{Y})$ 上のイデアルとする. ここで$\bar{X},\bar{Y}$はそれぞれ n 個の変数 $X_1,X_2,\ldots,X_n$ と m 個の変数 $Y_1,Y_2,\ldots,Y_m$を表す. $B(\bar{X})$ はブール環なので $B(\bar{X},\bar{Y})$ は係数環を $B(\bar{X})$ とする剰余環 $(B(\bar{X}))(\bar{Y})$ ともみなすことができる. $(B(\bar{X}))(\bar{Y})$ における Iのブーリアン・グレブナー基底を $G(\bar{X})$ で表す. このとき $G(\bar{X})$ は Iの comprehensive ブーリアン・グレブナー基底となる. すなわち$\bar{a}$を B の任意の n 個の要素とし, $I(\bar{a})=\{p(\bar{a},\bar{Y})|p(\bar{X},\bar{Y})\in I\}$ とおくとこれは $B(\bar{Y})$ のイデアルになるが, このとき $G(\bar{a})=\{g(\bar{a},\bar{Y})\mid g(\bar{X},\bar{Y})\in G(\bar{X})\text{ and }g(\bar{a},\bar{Y})\neq 0\}$ とおくと

定理 5

(1) $G(\bar{a})$ は $I(\bar{a})$ のブーリアン・グレブナー基底となる.

さらに任意の $f(\bar{X},\bar{Y})\in B(\bar{X},\bar{Y})$ にたいして

(2) $f(\bar{a},\bar{Y})\downarrow_{G(\bar{a})}=(f(\bar{X},\bar{Y})\downarrow_{G(\bar{X})})(\bar{a},\bar{Y})$ が成り立つ. □

6.5 応用

このセクションではブーリアン・グレブナー基底を用いた集合制約ソルバーの実行例をいくつか紹介する. 以下の例では/\は集合の積,\/は集合の和,~は補集合を, 小文字a1,a2,... は集合の要素, 大文

字S1,S2,...,X1,X2,... は集合を表す.

```
?- solve_set_element(A,B,C).
```

の A には集合制約が, B には解きたい集合変数, C には解きたい集合要素を変数として指定する (指定されない集合要素はすべて相異なる要素とみなされる). 最初に C が空の実行例を見る.

```
  ?- solve_set_element([
{a1,a9}/\(X2\/ ~X1)= {a2,a5,a7}/\S5,
S1/\(S2/\ ~{a5}\/(S3/\(S4/\ ~(X1\/{a6})))))=(S5/\S6)\/(S4/\S7/\S2)\/S8,
S5/\S4/\S9/\S6/\S2/\(S10\/X3\/{a7})/\({a9}\/X2)=0,S5/\S8/\ ~(X3\/{a5,a8})=0,
S2/\(~{a6,a8})=S4\/S8,S2/\(~{a9})=S11\/S10\/X2\/{a5,a7}\/S7,S11/\S3=0,
S10/\S3=0,S12=S9\/S7,S9/\S7/\S15/\ ~(X1\/X2\/X3\/{a4,a5,a6,a7,a8,a9,a10})=0,
{a4}/\S6={a4},X1/\S9=X1,X3/\S7=X3,S1\/S10\/X1\/X2=(S12\/S13)/\{a4}\/X2\/S10,
(S1\/S12\/S2)/\X1\/X2\/S6=(S10\/S9)\/(S7/\X3)\/S2,
(S5\/S3\/{a4})/\(S2\/S4\/S3\/S6)=(S1\/(X1\/X2/\(S3\/S10)))/\S1\/S14
],[X1,X2,X3],[]).
  contradiction deduced as follows
{a9} = 0
```

処理系は B を $\{a1, a2, \ldots\}$ の有限部分集合と有限部分集合の補集合全体から成るブール環として $\mathbf{B}(S1, S2, \ldots, X1, X2, X3)$ における

```
[{a1,a9\}/\(X2\/ ~X1)+{a2,a5,a7\}/\S5,
S1/\(S2/\ ~{a5\}\/(S3/\(S4/\ ~(X1\/{a6\})))))+(S5/\S6)\/(S4/\S7/\S2)\/S8,
S5/\S4/\S9/\S6/\S2/\(S10\/X3\/{a7\})/\({a9\}\/X2),S5/\S8/\ ~(X3\/{a5,a8\}),
S2/\(~{a6,a8\})+S4\/S8,S2/\(~{a9\})+S11\/S10\/X2\/{a5,a7\}\/S7,S11/\S3,
S10/\S3,S12+S9\/S7,S9/\S7/\S15/\ ~(X1\/X2\/X3\/{a4,a5,a6,a7,a8,a9,a10\}),
{a4\}/\S6+{a4\},X1/\S9+X1,X3/\S7+X3,S1\/S10\/X1\/X2 +(S12\/S13)/\{a4\}\/X2\/S10,
(S1\/S12\/S2)/\X1\/X2\/S6+(S10\/S9)\/(S7/\X3)\/S2,
(S5\/S3\/{a4\})/\(S2\/S4\/S3\/S6)+(S1\/(X1\/X2/\(S3\/S10)))/\S1\/S14]
```

のブーリアン・グレブナー基底を $[X1, X2, X3] < [S1, S2, \ldots, S14]$ なるブロックオーダーで計算し (解きたい変数が $X1, X2, X3$ なので) $X1, X2, X3$ のみを含む式を表示する. この実行例ではブーリアン・グレブナー基底に B の定数 $\{a9\}$ が含まれているので, 解が存在しない.

$a9$ が他の a_iのどれかと等しければ解が存在する可能性があるので $a9$ を変数として実行してみる.

```
  ?- solve_set_element([
{a1,a9}/\(X2\/ ~X1)= {a2,a5,a7}/\S5,
S1/\(S2/\ ~{a5}\/(S3/\(S4/\ ~(X1\/{a6})))))=(S5/\S6)\/(S4/\S7/\S2)\/S8,
S5/\S4/\S9/\S6/\S2/\(S10\/X3\/{a7})/\({a9}\/X2)=0,S5/\S8/\ ~(X3\/{a5,a8})=0,
S2/\(~{a6,a8})=S4\/S8,S2/\(~{a9})=S11\/S10\/X2\/{a5,a7}\/S7,S11/\S3=0,
```

```
S10/\S3=0,S12=S9\/S7,S9/\S7/\S15/\ ~(X1\/X2\/X3\/{a4,a5,a6,a7,a8,a9,a10})=0,
{a4}/\S6={a4},X1/\S9=X1,X3/\S7=X3,S1\/S10\/X1\/X2=(S12\/S13)/\{a4}\/X2\/S10,
(S1\/S12\/S2)/\X1\/X2\/S6=(S10\/S9)\/(S7/\X3)\/S2,
(S5\/S3\/{a4})/\(S2\/S4\/S3\/S6)=(S1\/(X1\/X2/\(S3\/S10)))/\S1\/S14
],[X1,X2,X3],(A9)).
  constraint is satisfiable when
(~{a2,a4})*{a9} = 0
--------------------------------
  under the above condition [X1,X2,X3] has the following form
({a5}*{a9}+{a5})*X3*X1 = 0
({a2,a5,a7}*{a9}+{a2,a5,a7})*X3*X2 = ({a2,a5,a7}*{a9}+{a2,a5,a7})*X3
({a2,a4}*{a9})*X3 = 0
({a1,a2,a4}*{a9}+{a1})*X1 = {a1,a4}*{a9}+{a1}
({a1,a2,a4}*{a9}+{a1})*X2 = 0
```

処理系はまず制約式の $\{a9\}$ を集合変数 $A9$ で置き換える. 次に $\mathbf{B}$ を $\{a1, a2, a3, \ldots\} - \{a9\}$ の有限部分集合と有限部分集合の補集合全体から成るブール環として $(\mathbf{B}(A9))(S1, S2, \ldots, X1, X2, X3)$ におけるブーリアン・グレブナー基底を $[X1, X2, X3] < [S1, S2, \ldots, S14]$ なるブロックオーダーで計算し定数部分 ($\mathbf{B}(A9)$ の要素) の $A9$ を $\{a9\}$ で再び置き換えた式を表示してから $X1, X2, X3$ のみを含む式を表示する. この場合 $a9 = a2$ あるいは $a9 = a4$ のとき解が存在して下の式の $a9$ にそれぞれ $a2$, $a4$ を代入したものが制約式の $a9$ にそれぞれ $a2$, $a4$ を代入して得られた制約式の解 (ブーリアン・グレブナー基底の $X1, X2, X3$ のみを含む部分) になることが定理 5 よりいえる.

実際に制約式の $a9$ をそれぞれ $a2$,$a4$ で置き換えて実行してみると,

```
  ?- solve_set_element([
{a1,a2}/\(X2\/ ~X1)= {a2,a5,a7}/\S5,
S1/\(S2/\ ~{a5}\/(S3/\(S4/\ ~(X1\/{a6}))))=(S5/\S6)\/(S4/\S7/\S2)\/S8,
S5/\S4/\S9/\S6/\S2/\(S10\/X3\/{a7})/\({a2}\/X2)=0,S5/\S8/\ ~(X3\/{a5,a8})=0,
S2/\(~{a6,a8})=S4\/S8,S2/\(~{a2})=S11\/S10\/X2\/{a5,a7}\/S7,S11/\S3=0,
S10/\S3=0,S12=S9\/S7,S9/\S7/\S15/\ ~(X1\/X2\/X3\/{a4,a5,a6,a7,a8,a2,a10})=0,
{a4}/\S6={a4},X1/\S9=X1,X3/\S7=X3,S1\/S10\/X1\/X2=(S12\/S13)/\{a4}\/X2\/S10,
(S1\/S12\/S2)/\X1\/X2\/S6=(S10\/S9)\/(S7/\X3)\/S2,
(S5\/S3\/{a4})/\(S2\/S4\/S3\/S6)=(S1\/(X1\/X2/\(S3\/S10)))/\S1\/S14
],[X1,X2,X3],[]).
{a5}*X3*X1 = 0
{a5,a7}*X3*X2 = {a5,a7}*X3
{a2}*X3 = 0
```

```
{a1,a2}*X1 = {a1}
{a1,a2}*X2 = 0
  ?- solve_set_element([
{a1,a4}/\(X2\/ ~X1)= {a2,a5,a7}/\S5,
S1/\(S2/\ ~{a5}\/(S3/\(S4/\ ~(X1\/{a6})))=(S5/\S6)\/(S4/\S7/\S2)\/S8,
S5/\S4/\S9/\S6/\S2/\(S10\/X3\/{a7})/\({a4}\/X2)=0,S5/\S8/\ ~(X3\/{a5,a8})=0,
S2/\(~{a6,a8})=S4\/S8,S2/\(~{a4})=S11\/S10\/X2\/{a5,a7}\/S7,S11/\S3=0,
S10/\S3=0,S12=S9\/S7,S9/\S7/\S15/\ ~(X1\/X2\/X3\/{a4,a5,a6,a7,a8,a4,a10})=0,
{a4}/\S6={a4},X1/\S9=X1,X3/\S7=X3,S1\/S10\/X1\/X2=(S12\/S13)/\{a4}\/X2\/S10,
(S1\/S12\/S2)/\X1\/X2\/S6=(S10\/S9)\/(S7/\X3)\/S2,
(S5\/S3\/{a4})/\(S2\/S4\/S3\/S6)=(S1\/(X1\/X2/\(S3\/S10)))/\S1\/S14
],[X1,X2,X3],[]).
{a5}*X3*X1 = 0
{a2,a5,a7}*X3*X2 = {a2,a5,a7}*X3
{a4}*X3 = 0
{a1,a4}*X1 = {a1,a4}
{a1,a4}*X2 = 0
```

6.6 おわりに

係数環がネーター環でいくつかの計算可能性に関する条件を満たすとき syzygy 基底の計算によって弱グブナー基底といわれるものが計算可能であることが知られている ([Trinks 78],[Zacharias 78]). ここで述べたブーリアン・グブナー基底はこの弱グブナー基底にほかならないが, 重要な点はそれが単項リダクションのみによって定義でき計算できる点である. これにより上の方法では実際に計算するのがほとんど不可能であったのが容易に計算できるようになった. また定理 3 と定理 4 によるアルゴリズムの改良は非常に有効である. 前節であげた最初の例では実際に計算された S 多項式は 4648 個であるのに対し計算しないですんだ冗長な S 多項式は 8621 個あった.

universal グブナー基底 ([Weispfenning 87]), すなわちすべてのアドミシブル全順序においてグブナー基底となるような基底も剰余環におけるブーリアン・グブナー基底においては著しく容易に構成できる. 剰余環においてはすべての変数の次数が高々1 なので項の数は有限個しか存在しないからである.

参考文献

[Aiba 88]Akira Aiba, Ko Sakai, Yosuke Sato, David J.Hawley, Ryuzo Hasegawa (1988). Constraint Logic Programming Language CAL Proceedings of The International Conference on Fifth Generation Computer, 263–276

[Buchberger 65]Buchberger, B. (1965). Ein Algorithmus zum Auffinden der Basiselemente des Restklassenrings nach einem nulldimensionalen Polynomideal. PhD thesis, Universität Innsbruck.

[Buchberger 85]Buchberger, B. (1985). Gröbner bases: An algorithmic method in polynomial ideal theory, chap 6 in Recent Trends in Multidimentional System Theory, N. K. Bose Ed., Reidel Publ. Comp.

[Rudeanu 74]Rudeanu, S. (1974). Boolean Functions and Equations, North-Holland

[Sakai 88]Sakai, K., Sato, Y. (1988). Boolean Gröbner bases. Proceeding of LA-Symposium in winter, RIMS, Kyoto Univ., 29–40

[Sakai 90]Sakai, K., Sato, Y., Menju, S. (1990). Boolean Gröbner bases(revised). ICOT Technical Report 613, also submitted for publication.

[Trinks 78]Trinks, W. (1978). Über B.Buchbergers Verfahren, Systeme algebraischer Gleichungen zu lösen. J.Number Theory 10, 475–488.

[Weispfenning 87]Weispfenning, V. (1987). Constructing universal Gröbner bases, Springer LNCS 356, 408–417.

[Weispfenning 89]Weispfenning, V. (1989). Gröbner bases in polynomial rings over commutative regular rings, EUROCAL '87, J.H. Davenport Ed., Springer LNCS Vol 378, 336–347.

[Weispfenning 92]Weispfenning, V. (1992). Comprehensive Gröbner bases, J.Symb.Comp.14/1,1–29.

[Zacharias 78]Zacharias, G. (1978). Generalized Gröbner bases in commutative polynomial rings. Thesis at M.I.T., Dept. Comp. Sci.

[Sato 93]佐藤洋祐, 毛受哲, 相場亮 (1993). ブーリアン・グレブナー基底の Syzygy 基底による特徴付け. 情報処理学会論文誌 Vol. 34 No 7 1549–1554